Anno 3 – N. 60
7/21 Ottobre 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

RICERCA e INVILUPPO

Uno degli ultimi virus è stato scritto da un programmatore in cerca di lavoro. Presso qualche azienda specializzata in antivirus. Bisogna dire che come curriculum è sicuramente originale. Più o meno come aggredire passanti con un'accetta per trovare un posto da infermiere. Come si può leggere qui a fianco, le polizie di mezzo mondo sono alla ricerca di una banda di pirati lituani che chiede soldi ai casinò online per non paralizzare il loro business con attacchi continuati.

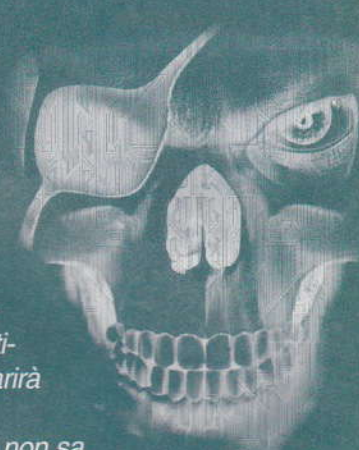
Pare che esista un mercato di zombie, computer controllati all'insaputa dei proprietari, da cui lanciare attacchi o anche banale spam. Ne metti insieme qualche migliaio e li puoi noleggiare al migliore offerente. Sono più stupidi quelli che non proteggono il loro computer o più criminali quelli che ne approfittano?

Microsoft ha finalmente pubblicato Service Pack 2. Settanta mega di aggiornamenti che possono diventare anche più di duecento, per gli amministratori di rete e per gli utenti avanzati. Dopo un giorno che SP2, "mirato alla sicurezza", era in distribuzione apparivano già su Internet i resoconti delle falle e delle vulnerabilità che l'aggiornamento non chiude, o apre. Intanto metà dei firewall non Microsoft smette di funzionare. Metà degli antivirus non Microsoft smette di funzionare. E non apparirà niente di meglio prima del 2006, sempre le cose a metà.

Il governo cerca di impedire la pirateria musicale. Ma non sa fare niente di meglio che pasticciare con il decreto Urbani. Non sanno di che cosa parlano, non sanno che cosa stanno facendo. Non sanno e intanto scrivono leggi sciocche. L'opposizione si oppone, senza sapere esattamente a che cosa e perché. Serve più ricerca. Ricerca di lavoro. Ricerca dei pirati. Ricerca sulla sicurezza. Ricerca di parlamentari competenti. Ricerca, ricerca, ricerca. A suon di ripeterla, la parola perde il proprio significato. Eppure senza ricerca non c'è sviluppo e senza sviluppo non andiamo da nessuna parte.

Noi hacker siamo chiamati alla ricerca. Saremo i motori dello sviluppo. Si tratta solo di superare un po' di ostacoli, dai programmatori di virus ai banditi lituani a Microsoft, fino a quanti siedono in Parlamento.

Uno per volta, ne siamo certi, gli ostacoli cadranno. Restiamo uniti e sotto con l'hacking!

theguilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Boss: TheGuilty@hackerjournal.it

I ragazzi della redazione europea: Il Coccia, Bismark.it, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron Silvio De Pecher, Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Bacco" Colombo, Elena "Super Fanta Menosina" Varesi

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Copertina: Daniele Festa

Publishing company: 4ever S.r.l. Via Torino, 51 20063 Cernusco S/N (MI) Fax +39/02.92.43.22.35

Printing: Roto 3

Distributore: Parrini & C. S.PA. 00189 Roma - Via Vitorchiano, 81 Tel. 06.33455.1 r.a. 20134 Milano, V.le Forlanini, 23 Tel. 02.75417.1 r.a.

Abbonamenti: Staff S.r.l. Via Bodoni, 24 20090 Buccinasco (MI) Tel. 02.45.70.24.15 Fax 02.45.70.24.34 Lun. - Ven. 9,30/12,30 - 14,30/17,30 abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

DDoS su LARGA SCALA

Distributed Denial of Service: l'arte di mandare in blocco una rete intera. Per esempio, un mese fa...

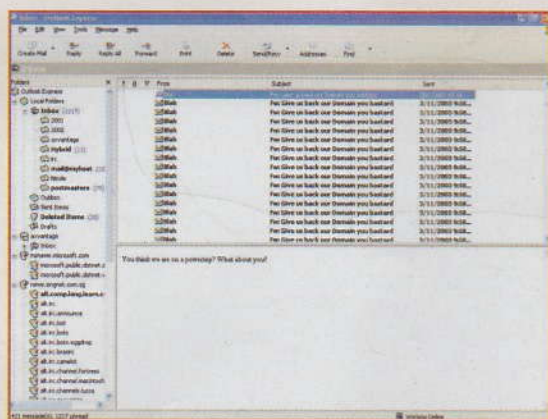
Alice Springs, Australia, otto settembre. 35 mila cittadini restano scollegati da Internet per cinque ore. Non è un incidente, ma un attacco premeditato. Quello che è peggio, emerge che l'attacco è opera di bande di pirati lituani, che attaccano e poi chiedono soldi per non ripetersi.

Una vera e propria estorsione, con Telstra, la compagnia telefonica australiana fornitrice dei collegamenti Internet nella zona, che lascia passare molte ore prima di ammettere che sì, c'è stato un attacco e doppio sì, i suoi server non hanno retto.

Non si tratta di un episodio isolato: nello stesso periodo si è verificata un'epidemia di attacchi di questo tipo contro società titolari di casinò online. Una di queste, Sportbetting, si è rifiutata di pagare il vero e proprio pizzo chiesto dagli estorsori e ha subito gravi danni al proprio business per via dei continui attacchi.

◄ I casinò online sono le vittime preferite dei ricattatori del DDoS.

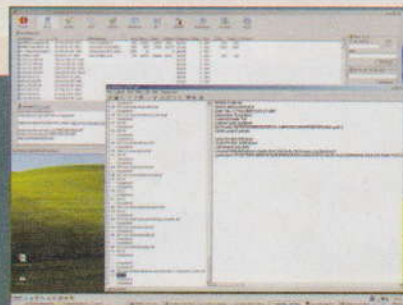
Il fenomeno non è ancora sotto controllo; le polizie internazionali collaborano e sono arrivati i primi risultati, ma da questo punto di vista il cyberspazio resta tuttora far west. Una delle scoperte più sconvolgenti da questo punto di vista è l'esistenza di un mercato nero di zombie: PC compromessi da attacchi esterni e controllabili remotamente dai pirati. Ne mettono insieme anche qualche migliaio e li noleggiano a chi vuole condurre un attacco dietro compenso di diecimila o ventimila dollari. Attraverso i PC compromessi partono migliaia di attacchi ed ecco che i server della vittima sono in ginocchio.

► Una variante del DDoS è il mailbombing: inviare sul bersaglio una quantità di posta insostenibile per il suo server.

Una ragione in più per stare attenti alla sicurezza dei nostri PC. A parte il fatto che sono nostri e non di qualche cracker bielorusso o azero, se vengono compromessi possono essere usati per commettere atti criminali a nostra insaputa. E dimostrare che non ne sappiamo niente non sarà così semplice, senza contare la figuraccia.

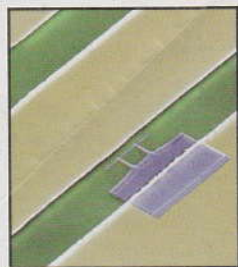
ZOMBI ALL'UNO PERCENTO

Secondo l'istituto di ricerca Sandvine, l'uno percento di tutti gli host attivi su Internet potrebbe essere stabilmente compromesso e usato per inviare spam o attaccare altri server. Molta gente non lo sa, ma invia – involontariamente – più spam di quello che riceve.

CHE COS'È UN DDOS

DDosS: Distributed Denial of Service, servizio negato in modo distribuito. Attacco in cui una moltitudine di sistemi compromessi bombarda suo malgrado un bersaglio, che collassa sotto l'alto numero di pacchetti in arrivo e così non riesce a servire gli utenti legittimi.

HOT!

COMPUTER E SEGRETI DEL FUTURO

Hanno sparato un solo fotone (la più piccola particella di luce) su un solo atomo di un superconduttore e ne hanno fatto venire fuori una nuova sostanza, una nuova e piccolissima molecola artificiale, con la base lunga circa 9 milionesimi di millimetro. Non sanno ancora se chiamarla Quton oppure Phobit, ma la sostanza è la stessa: è più vicino il momento in cui si potranno realizzare sistemi di elaborazione quantistici e potentissimi mezzi di cifratura. Il massimo che l'attuale conoscenza tecnologica ci offre in tali settori. Tutto questo grazie ai ricercatori dell'Università di Yale.

SASSER SULLA TESTA DEL SUO CREATORE

Una bella tegola che si è tirato addosso: il 18 enne Sven Jashan, tedesco, deve rispondere di aver creato e fatto circolare il virus Sasser, ancora in cima alla classifica dei virus potenzialmente più pericolosi in circolazione.
Il ragazzo è accusato di avere infettato circa 18 milioni di pc in tutto il mondo e di avere creato danni per almeno 130 mila euro, derivanti dalle 143 denunce a suo carico provenienti dalle società più importanti. Rischia cinque anni di carcere. Su di lui Microsoft aveva posto una taglia di 250 mila dollari!

APPLE: BATTERIE INCENDIARIE

Tutte le batterie vendute da gennaio 2004 ad agosto 2004 e destinate all'uso con i computer portatili PowerBook G4 da 15" (Aluminum), fabbricate in Corea del Sud, devono essere sostituite per pericoli di surriscaldamento con possibile conseguente incendio.
Come facciamo a sapere se abbiamo in casa un piromane sotto le spoglie di un PowerBook 15" Apple? Guardiamo il codice del prodotto, stampato direttamente sulla batteria. Le batterie che dovremo sostituire, hanno codice prodotto A1045 e numero di serie che inizia con HQ404, HQ405, HQ406, HQ407 oppure HQ408. Il codice prodotto e il numero di serie sono impressi sull'etichetta posta sul fondo della batteria e sono visibili quando questa viene rimossa dal computer. Il numero di serie è stampato in caratteri neri sotto il codice a barre.
L'etichetta posta sul fondo della batteria riporta le seguenti diciture: "15-inch PowerBook G4 Rechargeable Battery" e "Model No: A1045".

BELLISSIMO, DA INCENDIARE IL CUORE

IMPRONTE DIGITALI E MICROSOFT

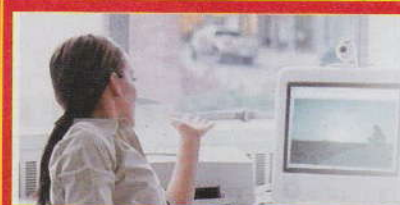
Non è certamente una novità tecnologica. Già da molto tempo esistono i lettori di impronta digitale, che ci evitano di scrivere nome utente e password per le centinaia di volte necessarie per raggiungere i diversi servizi a cui vogliamo accedere. Si memorizza una volta sola e poi si appoggia il dito su una piastrina che legge la nostra impronta, tutte le volte che ci viene richiesto il nome e la password. Microsoft introduce in questi giorni sul mercato la sua versione dell'aggeggio, che sarà integrato nella tastiera, nel mouse oppure sarà venduto come accessorio separato. Il vero problema è che, a detta della prestigiosa rivista Wired che ha provato il sistema in anteprima, come tutti i prodotti Microsoft la configurazione del sistema è macchinosa e richiede riavvii del computer. Per cui diventa tutto più complicato ed è sufficiente che sia un altro utente a dover usare il computer che iniziano i guai. Per di più utente e password saranno sempre memorizzati, seppure cifrati, nel pc, invece che nella nostra mente.
Come essere sicuri che Windows ne protegga davvero la segretezza? Un metodo semplice e sicuro come un key file su chiavetta Usb asportabile è, forse, un metodo migliore che andrebbe diffuso.

PARLA CON ELOISA

All'URL www.eloisa.it troviamo, anche se la definizione è riduttiva, la versione attuale del vecchissimo programma Eliza, capace di interloquire con l'utente. La capacità di aggiornare le risposte

e di costruire una conversazione che ha un'apparenza quasi sensata è decisamente migliorata, naturalmente.
I creatori ovviamente non sono gli stessi di allora. Insomma, tutto nuovo, ripensato, aggiornato al web e ai collegamenti on-line. Un gioco molto divertente, che costa qualche decina di euro e non vale la pena acquistare, salvo che si vogliano stupire gli amici a colpi di brevi sessioni di circa venti minuti. Oltre, diventa un'ossessione.

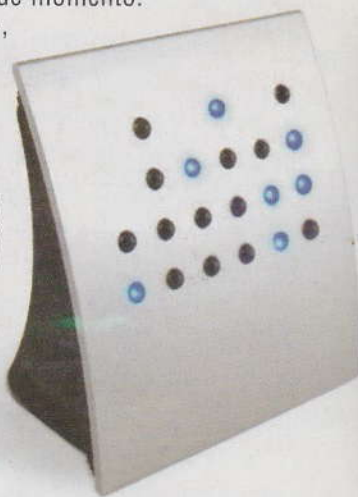
TARIFFE ADSL: DODICI VOLTE PIÙ CARE

Peschiamo a caso un'offerta Adsl italiana e una francese, dello stesso operatore: Telecom. In Italia la connessione a 1 Mb/s costa 64,95 euro al mese. In Francia? 5,48 euro al mese. Sì, avete letto bene: sessantaquattro e rotti contro cinque e rotti. Noi italiani paghiamo circa dodici volte di più la stessa connessione dei francesi. Gli altri operatori non si fanno bagnare il naso e anche loro ce la mettono tutta per spillarci quattrini in misura di almeno il doppio dei francesi. Per non parlare di offerte nemmeno confrontabili, come quella a 3 Mb/s di Telecom francese a 12,48 euro/mese.
Eppoi ci vengono a raccontare che bisogna dare a tutti la possibilità di collegarsi, che lo sviluppo del mezzogiorno passa attraverso le infrastrutture telematiche, che agli studenti deve essere data la cultura informatica a tutti i costi...
Comunque, se vogliamo farci sentire, possiamo sempre firmare la petizione all'indirizzo http://www.petitiononline.com/adsl04it/petition.html

LA TROTTOLA INTELLIGENTE

Ci ricordiamo del gioco della trottola, vero? Una spintarella a un disco più o meno colorato e si stava lì a guardare assorti un pezzo di metallo girare come un pazzo. Ecco, un po' pazzo deve essere anche quello che ha inventato la trottola a LED, capace di formare scritte diverse sfruttando la persistenza dell'occhio umano. Si chiama iTop e un chip interno consente di scegliere tra 8 livelli di gioco e tra i più divertenti troviamo il livello mistico, ovvero la risposta a qualunque nostra domanda, tramite un sì e un no che si formano magicamente sotto i nostri occhi. Oppure il livello che indica, con lo stesso sistema, la velocità a cui siamo riusciti a fare girare la trottola, in giri per minuto. Per 12 dollari, da non perdere.

HOT!

OROLOGIO BINARIO

L'orologio che possiamo leggere solo noi (e pochi altri...): è l'orologio binario. Al posto delle lancette i led colorati disposti su righe e colonne. Sulle righe i pesi, sulle colonne i valori. Una semplice addizione e saprete l'ora precisa in qualunque momento. Semplice, no? Costa solo circa 20 o 30 dollari (idem in euro) secondo il colore.

DIGITALE DA 007

150 foto con la risoluzione di 640 x 480 pixel: o il doppio alla metà. È la macchina fotografica di 007, che sta in un accendino. 99,99 dollari su http://www.amazon.com e un po' di divertimento assicurato. Peraltro fa delle foto decisamente buone. In situazioni difficili e per le nostre attività di ingegneria sociale, niente di meglio.

HACKING DEL DIESEL

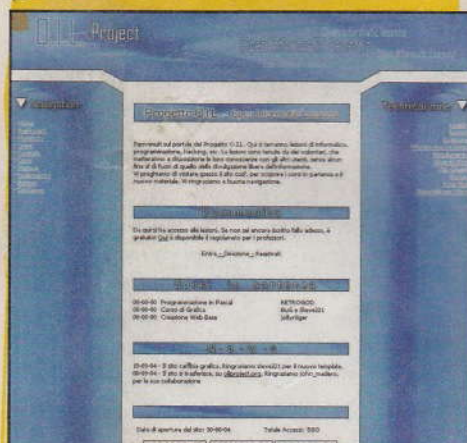
Gli hacker non esistono solo nell'informatica: si tratta di un dogma che ben conoscete. Spaziare su più argomenti è in se stesso una sorta di hacking. In breve: esiste la possibilità di usare, nei motori diesel, l'olio di semi al posto del gasolio, senza apportare assolutamente alcuna modifica al motore. Io già lo faccio con ottimi risultati, miscelando 1/3 di gasolio e 2/3 di olio di semi vari, il cui costo, inferiore ai 70 eurocent al litro, è ben inferiore a quello del gasolio. Non uso l'olio di semi puro per problemi di fluidità: alle basse temperature tende a brinare, con il rischio di otturare gli iniettori. La miscela da me usata è ottimale, consentendo di mantenere un'eccellente fluidità della miscela e di risparmiare svariati euro a ogni pieno. Cerco qualcuno in grado di dirmi se esiste un modo casalingo per rompere le molecole più lunghe dell'olio di semi, in modo da garantirne la fluidità senza miscelarlo con il gasolio.

Poppy

Ehm, cosa ti ha detto il meccanico l'ultima volta che hai fatto il tagliando? ;) E il numero di ottani? E i battiti in testa? E le scorie? E la marmitta catalitica? E i prodotti di combustione che respireremo? Giriamo l'appello ai lettori e invitiamo a scriverci: vi interessa l'hacking... chimico? Tutto quello che è possibile fare con gli ingredienti che trovate in cucina, per esempio. Perplessi... attendiamo risposte.

L'OPEN-SOURCE DELLA FORMAZIONE?

Nasce il progetto OIL (Open Informatic Lessons) che ha come obiettivo principale quello della libera divulgazione delle conoscenze, al fine di arricchirsi a vicenda di preziose informazioni e nozioni che spaziano nell'immenso settore informatico. Le lezioni gratuite online, che trattano di programmazione, hacking, grafica, linux e creazione siti web, sono tenute da volontari. È la mentalità open-source applicata alla formazione. Se siamo interessati facciamo un salto su www.oilproject.org.

Madero OIL project

Ragazzi, l'idea è bellissima e in pieno spirito hacker. Continuate così e teneteci informati.

EPSON 1

Riguardo alla risposta della Epson nella persona del direttore commerciale. Mi piacerebbe porre un ulteriore interrogativo al signor Ascari. Sforzandomi, riesco a credere a quello che dice. Ma se allora è, mi spiega il motivo tecnologico che spinge Epson a non permettere la stampa solo con colore nero se la cartuccia a colori è esaurita? Con tutte le tecnologie che Epson è in grado di sviluppare, non è in grado di disabilitare il funzionamento della testina a colori in qualche modo? Sono un affezionato acquirente di vostre stampanti, ma non di vostre cartucce, e non lo sarò mai. Spero publicchiate il mio pensiero , anche se in forma ridottissima.

L0sc0

Tagliato, per ragioni di spazio. Ma il senso è stato mantenuto. Toc, toc: Epson, se ci sei, batti un colpo!

EPSON 2

Ho comprato casualmente la vostra rivista, e ho scoperto che il primo articolo su Epson era proprio ciò che cercavo. Al di là delle risposte Epson che sono le stesse che hanno dato a me, mi pare veramente...
Un'altra cosa che ho scoperto per esempio sulla mia Epson stylus photo edition C64 è che se un colore è finito, tutta la stampante non funziona. E' una cosa veramente incredibile, senza contare il fatto che 25 € di cartuccia per poche stampe è veramente vergognoso. Purtroppo non ho visto il precedente articolo, quello che parlava di come resettare le cartucce.

Sauro

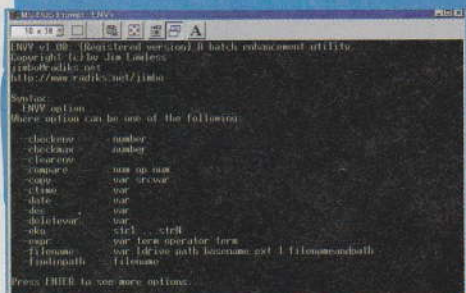
Tagliato anche il testo di Sauro, che ci scuserà. La domanda è sempre la stessa: perché, se ho finito un colore, tutto il resto si deve fermare? Perché, se ho finito solo il blu,

devo buttare anche il giallo e il rosso?
Perché, con tutta la tecnologia di cui tutti si vantano, non si spende qualcosina in più per evitare di spennare gli utenti? (ci siamo forse dati una risposta implicita?...)

INFO SUL DOS

Volevo anche chiedere un'informazione inerente ai comandi in DOS. Io ne conosco pochissimi, per sopravvivenza, come DEL, DELTREE, FORMAT ecc., e volevo chiedervi dove era possibile avere info sui vari comandi. Siete forti davvero.

Jeff

Vuoi DOS? E DOS avrai: http://www.easydos.com/

SITO ANONIMO: UTOPIA?

*Vorrei chiedere a un vostro esperto un parere per costruire un sito anonimo. Un mio amico ha già un sito con del materiale culturale. Si è registrato e ha un regolare sito *.com. (quindi non anonimo). Ha la possibilità di inserire nel suo spazio altri indirizzi. Il problema dell'anonimato sta nel fatto che si vorrebbe non fosse possibile risalire all'autore o al proprietario del sito stesso.*
Abbiamo in mente niente di illegale, ma solo motivi di privacy [seguono i motivi, abbastanza fondati. N.d.R.] È possibile fare questo?

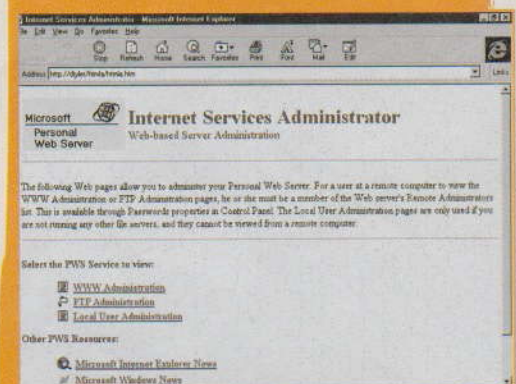
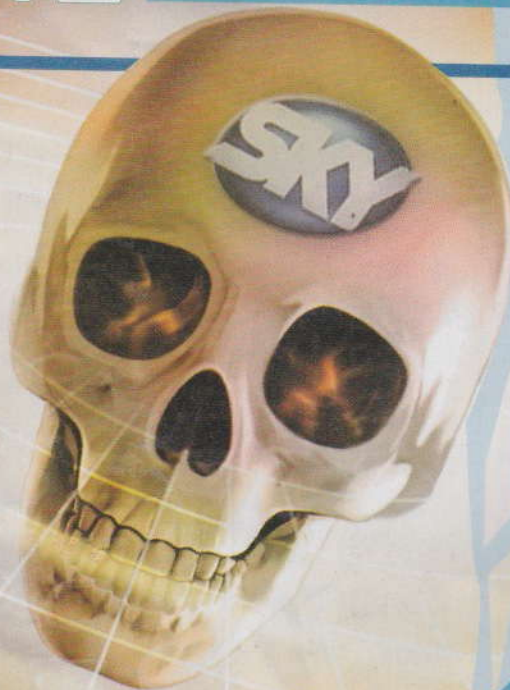
§ Altair §

Nisba, caro § Altair §. Per registrarvi il nome di dominio qualunque provider autorizzato deve avere dei precisi riferimenti che, al momento della richiesta, non possono risultare fasulli. Quindi tramite una qualunque interrogazione whois chiunque può risalire all'intestatario. E allora, come fanno quelli che mettono materiale illegale su Internet, a non farsi beccare? Qui si sconfina verso i limiti della legalità. In genere, infatti, i domini sospetti sono sempre intestati a società e quindi una semplice interrogazione whois porta solamente a fantasiosi nomi, collocati in luoghi del mondo assolutamente improbabili. Ed è sempre ben più complicato risalire ai veri intestatari di una ragione sociale registrata chissà dove. Per togliervi il dubbio: qui troviamo i servizi whois di quasi tutte le nazioni del mondo: http://www.101domain.com/domain_whois_server.php

PWS SU XP HOME?

Sono disperato! Aiutatemi! Ho acquistato un pc con il buon (?) Windows XP Home. Anche perché Professional non te lo propongono nemmeno, se sei un privato. Lo porto a casa e cosa mi accorgo? Che non è installato un server! E io adesso come faccio a provare i miei esperimenti in ASP? Devo prendere una macchina apposta con Windows2000, che aveva tutto per tutti senza storie? Aiutatemi!

Kilimangiarò

C'hai ragione. È la vera fregatura della versione Home: non ha il personal web server. Come fare? Qualcosa in rete si trova. Ma è una procedura piuttosto complessa e non sempre riesce al primo colpo. Richiede anche un CD con i file di Windows 2000. Quelli di XP Pro non servirebbero a nulla. Si tratta, in sostanza, di un trucco per aggiungere i file che mancano e aggirare alcune protezioni che XP mette in atto. Di più riusciremo a dirti in un apposito articolo, prossimamente: nella posta c'è poco spazio. Ma se fai una ricerca...

Ecco tutto quello che non dovremmo mai fare, ma che qualcuno sta facendo lo stesso. A suo rischio e pericolo e... inutilmente. A fine anno, infatti, tutti i giochi saranno chiusi.

Truffa a SKY:

Da un po' di tempo le voci circolano nelle chat e nei forum: Sky si può vedere a sbafo con le carte pirata, facilmente acquistabili su Internet o nel negozio d'elettronica sotto casa. Ma è tutto vero?
Facciamo subito chiarezza: lo standard utilizzato fin'ora, il Seca2, non è stato craccato e l'algoritmo non è ancora conosciuto. Esistono infatti due tipi di card: quelle che usano la versione A del Seca2 (card chiamate in gergo "bianchine") e quelle che usano la versione V7.0B (chiamate in gergo le "azzurrine"). I provider che usano la versione B dello standard, ovvero quella adottata dalle "azzurrine", non sono ancora vittime della pirateria degli emulatori.
Per aprire il Seca2 è comunque disponibile una grande varietà di dispositivi:

si rischiano GUAI SERI!

Se proprio vogliamo vedere le partite di cartello a sbafo, teniamo presente che i canali esteri che trasmettono la Serie A sono molti e alcuni usano codifiche aperte. L'elenco delle partite e i relativi canali sono facilmente rintracciabili su Internet: l'unico problema è che dobbiamo sopportare il commento in qualche lingua strana.
Del resto se vogliamo vedere a sbafo, a qualcosa dovremo pure rinunciare, no?

programmi per pc con scheda satellitare, firmware per CAM programmabili, firmware modificati per Gold Box e per altri decoder e le famose smart card.
Tra le smart card la più conosciuta è la Titanium, card usata da tempo nei sistemi per controllo degli accessi e da qualche mese salita agli onori della cronaca come "la carta che apre Sky". Venduta a un prezzo vicino ai 60 euro si programma con lo Smartmouse, apparecchio che via seriale permette la programmazione delle smart card, scaricando appositi file, che possiamo facilmente recuperare sui siti e sui bot delle chat dell'underground satellitare.

Smartmouse lo troviamo a un prezzo tra 15 e 20 euro, ma può essere agevolmente auto costruito tramite schemi che si trovano facilmente, sempre nella Grande Rete. Cerchiamo su Google la parola "smartmouse" e troviamo ogni indicazione in merito. Ultimamente sono usciti altri tipi di card: come la Platinium e la Knotcard… Usano dei file specifici e vengono programmate sempre con il solito smartmouse.

I firmware modificati per Gold Box, i vecchi decoder Seca ufficiali di Tele+, sono invece un'altra storia. Tali firmware, oltre a permettere la visione a scrocco di Sky trasformano in splendidi cigni dei decoder nati come brutti anatroccoli (solo 999 canali, senza supporto al DISEQC, senza dual feed). Questo tipo di modifica non è disponibile per tutti i Gold Box e alcuni modelli usano firmware in comune con altri.
Quindi fino ad ora le possibilità di vedere Sky senza pagare sono molteplici e, seppure illegali, sono alla portata di tutte le tasche, ma…

Sky, la vendetta

Sky naturalmente non sta a guardare e la vita per chi usa gli emulatori non è facile, anzi! Oltre la chiusura del Seca2 con il passaggio al nuovo standard NDS (questione già trattata in passato da HJ), Sky adotta contromisure prima di ogni partita di calcio, mettendo al buio i portoghesi per qualche giorno tramite la riprogrammazione dell'Ecm (la chiave di decrittazione). Le modifiche avvengono circa un'ora e mezzo prima di ogni partita, e non sono semplici cambi di chiavi (peraltro inutili, in quanto tutti gli emulatori si autoaggiornano), ma veri cambiamenti nella comunicazione tra decoder e card, che mettono al buio tutti i dispositivi emulatori per alcuni giorni senza possibilità di appello.

▲ *Programmazione? Un gioco da ragazzi. Ma è illegale e non ne vale più la pena.*

Se pensiamo (e in molti lo pensavamo prima dell'inizio del campionato) che questo tipo di contromisura non possa essere effettuata ogni settimana, ci sbagliamo di grosso: ci sono 54 tipi di comandi possibili, per cui da qui a dicembre ogni partita avrà la sua contromisura.

Ma qualche giorno è anche il tempo necessario affinché venga studiata una soluzione... e così il gioco a guardie e ladri continua... Anche se è comunque una partita sbilanciata a favore di Sky, perché i primi file che vengono rilasciati nel mercato clandestino non sempre vanno bene per il proprio ricevitore: non è più come ai tempi di Tele+ in cui c'erano solo Gold Box e Aston, adesso la varietà di CAM (il modulo d'accesso condizionato) e di ricevitori è impressionate, e ci sono spesso problemi di compatibilità.

I file killer

Un fenomeno che colpisce i possessori di Titanium è anche quello dei killer file, file che cancellano il sistema operativo della card e un parametro di funzionamento chiamato ATR (Answer To Reset) rendendola inservibile. Naturalmente esistono metodi per rianimarle, ma non sempre funzionano.

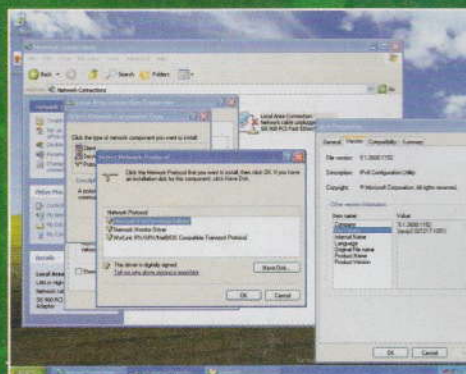
Soldi buttati

Se vogliamo acquistare qualche dispositivo per vedere a scrocco le partite di Sky il consiglio è uno solo: non facciamolo, e andiamo a vederci le partite al bar. Prima di arricchire qualche commerciante senza scrupoli, pensiamoci bene: il nostro portafoglio e i nostri nervi ringrazieranno. E teniamo in considerazione che entro breve Seca2 sarà chiuso, e NDS2 non è una codifica facilmente apribile. Anzi...

Mirco Ongaro

L'aggiornamento più IMPORTANTE

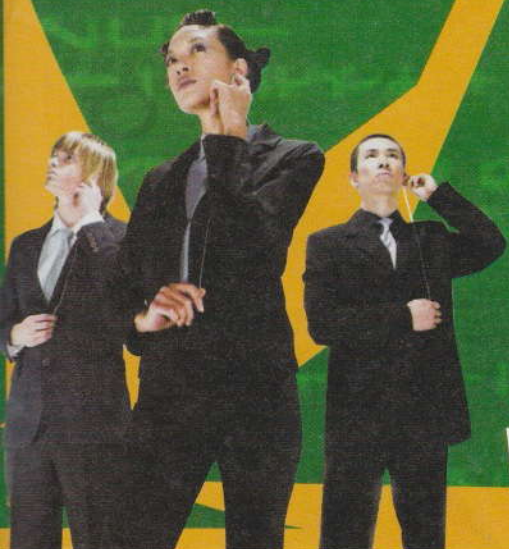
Le cose fondamentali da sapere sull'ultimo grande aggiornamento di Windows Xp da qui al 2006 e forse oltre

Chiamarlo aggiornamento è poco. La versione base supera gli ottanta mega, quella completa di tutto oltrepassa i duecento. Service Pack 2 è veramente una revisione fondamentale di Windows, che contiene una marea di aggiornamenti per la sicurezza e altrettanti problemi di compatibilità. Quindi non può essere ignorato e contemporaneamente bisogna installarlo con attenzione. Ecco perché.

▲ *Service Pack 2 cambia le cose anche a livello di impostazione dei collegamenti di rete.*

IE: uguale ma più sicuro

Chi si aspettava nuove funzioni nell'ormai stravecchio Explorer troverà solo novità di sicurezza. Il blocco dei pop-up è abilitato di serie e viene disabilitata l'installazione automatica dei Browser Help Object (BHO). I BHO sono stati usati per arricchire Explorer di nuove funzioni, ma anche per abusare del PC del proprietario in tutti i modi concepibili. Gli script, inoltre, non potranno più cambiare le impostazioni della finestra del browser.

Posta: qualcuno cambierà programma

Nel nome della sicurezza, Outlook blocca le mail HTML che contengono immagini o allegati sospetti, tipo .exe. Non è possibile imposta-

IN ATTESA DELL'INTERMINABILE

Longhorn sarà la nuova versione riveduta e corretta di Windows e la sua data di rilascio è stata sempre alquanto incerta. Microsoft dice che arriverà entro il 2006, ma contemporaneamente è stato annunciato che alcune tecnologie di base (compreso il nuovo sistema di gestione dei file, WinFS) non saranno sviluppate in tempo. Morale: un Service Pack 3 non dovrebbe arrivare e SP2 sarà l'ultima grossa revisione di Windows fino al 2006. Ma non scommettiamoci troppo.

re una whitelist che autorizzi nostro cugino programmatore a mandarci le sue utility, quindi è una opzione che verrà amata od odiata secondo i gusti.
Una nuova API detta Attachment Execution Service (AES) effettua controlli ulteriori sugli allegati ritenuti pericolosi e se lo ritiene necessario avvia automaticamente l'antivirus di sistema.

Il firewall si accende

L'Internet Connections Firewall (ICF) di Windows XP ritorna in versione aggiornata e potenziata con il nome di Windows Firewall. Soprattutto in versione accesa, dato che di serie il precedente firewall era spento. Prima era impossibile impostare regole di traffico riguardanti singole applicazioni mentre ora si può, anche su base temporanea.

Si aggiorna da solo

L'aggiornamento automatico di SP2 può essere attivato parzialmente o totalmente. Nel secondo caso le patch di sistema vengono scaricate in automatico sfruttando la banda non utilizzata. Chi attiva in modo parziale e quindi decide se aggiornare o meno riceverà notifiche periodiche dello stato di rischio del proprio computer. Una nuova funzione provvederà a installare automaticamente prima dello spegnimento del computer gli aggiornamenti critici di cui è stato fatto lo scaricamento.

Questa novità permette di governare antivirus, firewall e aggiornamenti automatici in modo centralizzato. È anche la responsabile di una marea di incompatibilità con programmi indipendenti che svolgono queste funzioni. Uno degli effetti collaterali di SP2 è che

▲ *Il Centro sicurezza del nuovo Windows dopo la cura Service Pack 2 si occupa di antivirus, firewall e aggiornamenti automatici.*

molti programmi non funzioneranno e si dovrà attendere una patch dai loro produttori.

Memoria protetta

Una tecnologia hardware di nome NX (No eXecute), che rafforza la separazione tra le aree di memoria e limita il raggio di azione di codice aggressivo, viene riconosciuta da SP2 tramite la tecnologia software DEP (Data Execution Prevention). Questo ridurrà fortemente le vulnerabilità del sistema, ma costringerà molti programmi a essere riscritti per poter funzionare. Vedremo ancora schermate che ricordano il famigerato Blue Screen of Death, ma ora il sistema resterà con il controllo della situazione.

Un modo nuovo di usare Windows

Non è una nuova versione di Windows, ma i cambiamenti sono veramente tantissimi (abbiamo lo spazio per citare solo i più significativi). La sicurezza totale del sistema dovrebbe essere nettamente migliorata; tuttavia si pagherà un altissimo prezzo iniziale in incompatibilità del software indipendente e nel doversi abituare a novità come il Centro sicurezza.

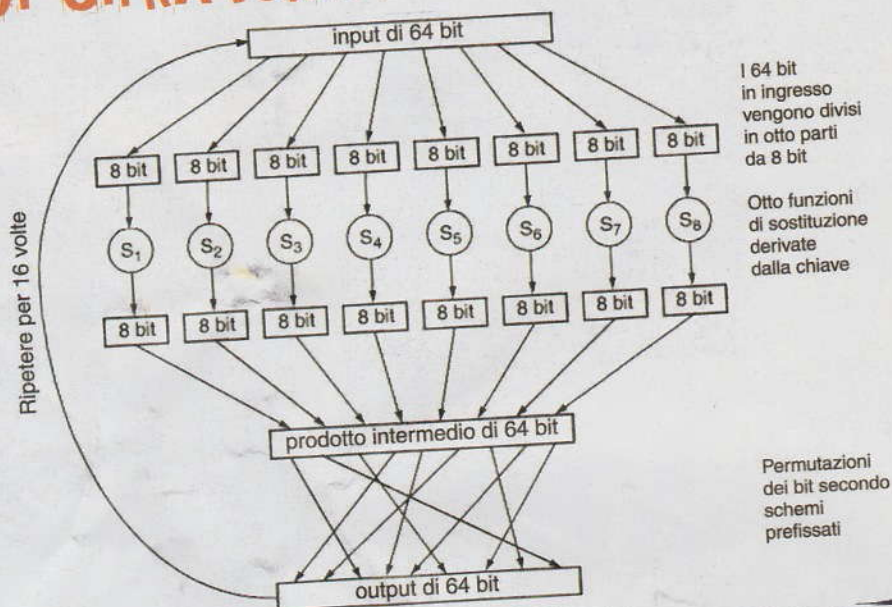
Proteggi il tuo PC da virus, hacker e worm. - la homepage del sito Microsoft su Service Pack 2

Consigliamo di leggere la documentazione disponibile sul sito Microsoft prima di optare per l'aggiornamento. Consideriamo che non è un semplice upgrade e anche la sola installazione richiederà molto tempo, quindi lanciamola solo se non siamo di fretta.

L'ABC di DES

Un conto è la crittografia a chiave pubblica, quella di PGP e altri programmi. Un conto è la crittografia a chiave segreta, quella che serve meno a scambiare file cifrati con il mondo ma è utilissima per proteggere le nostre cose. Che cosa c'è sotto? Come funziona? Vediamo, in breve ma con precisione, come funziona l'algoritmo di cifratura DES. In prossimi articoli affronteremo anche altri algoritmi, più complessi e più sicuri.

Il concetto di blocco

La cifratura avviene su blocchi del file da cifrare. Ogni sistema ha la sua misura di blocco, ma in generale sono cose tipo 64 bit. La cifratura teorica dovrebbe funzionare in questo modo: per ogni blocco si prende ciascuno dei 2^64 valori di input possibili e lo si fa corrispondere a uno e uno solo dei 2^64 valori di output possibili. Ma non è pratico, dal momento che l'operazione richiederebbe (2^64)*(64)=2^70 bit. Troppi (provato a vedere quanti sono?). Per questo i sistemi di cifratura correnti non fanno così, ma adottano invece una chiave di lunghezza ragionevole (per esempio 64 bit) e generano una mappatura uno-a-uno che, a chi non sa la chiave, risulta completamente casuale rispetto al file di partenza.
Le operazioni che vengono comunemente

eseguite sui blocchi sono di due tipi: sostituzione e permutazione. Nella prima, specifichiamo l'output k per ciascuno dei possibili valori 2k dell'input. Nella seconda, per ognuno dei k bit di input, specifichiamo la posizione di output in cui deve andare.
Se per ora sembra arabo non c'è da preoccuparsi: abbiamo esempi pratici da qui a poche righe!

ESEMPIO DI UN SISTEMA DI CIFRATURA A BLOCCHI

Ecco un esempio di un sistema di cifratura a blocchi a chiave segreta con procedura di sostituzione e permutazione. L'input iniziale di 64 bit viene suddiviso in parti da otto bit ciascuna. La chiave viene incrociata con ciascuna porzione di otto bit e il risultato sostituisce i bit originali. I 64 bit risultanti vengono scambiati di posizione, in un processo di permutazione. Il risultato finale è la cifratura dei 64 bit iniziali. Il processo viene ripetuto a 64 bit per volta fino a fine file. La procedura descritta può essere ripetuta più volte, in più round, ogni volta partendo dall'output del round precedente. E adesso vediamo come funziona un sistema di cifratura vero come DES. Per decifrare il file bisogna eseguire, ovviamente a rovescio, le stesse operazioni.

◀ *La scheda madre di DES Cracker, il primo computer a violare la sicurezza di DES.*

Data Encryption Standard (DES)

Nel DES i blocchi hanno lunghezza di 64 bit. Otto bit però vengono usati per il controllo degli errori. Ogni bit di controllo fa riferimento a otto bit del blocco; ogni blocco deve avere parità dispari, ossia contenere un numero dispari di bit. Solo 56 bit, genera-

Prendiamo l'algoritmo di cifratura DES e smontiamolo pezzo per pezzo!

ti casualmente, pesano effettivamente sulla cifratura. Questo ne fa un sistema non sicurissimo, che già nel 1998 un computer da 220 mila dollari ha violato nel giro di 56 ore, mentre l'anno dopo si è ottenuto lo stesso risultato con una rete di alcune migliaia di personal computer che destinavano il loro tempo macchina libero alla sfida. La sua variante Triple DES è 2^56 volte più sicura e infatti oggi è molto più utilizzata.

In DES ogni blocco da cifrare viene sottoposto a una permutazione iniziale detta IP, poi a una serie di sostituzioni dipendenti dalla chiave e infine a una permutazione finale IP-1 inversa alla precedente. La permutazione iniziale IP ha questo schema:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Sembrano le estrazioni del lotto ma invece è ancora più semplice. Il primo bit della permutazione sarà il bit numero 58 della sequenza iniziale. Il secondo bit sarà il numero 50, il terzo sarà il numero 42 e così via. Il penultimo bit sarà il numero 15 della sequenza di inizio e l'ultimo bit sarà il numero 7. La permutazione finale, IP-1, sarà invece la seguente:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

▲ *Uno dei processori di DES Cracker, la macchina ammazzaDES.*

Lo schema è lo stesso. Il primo bit della sequenza finale sarà il numero 40 della sequenza in ingresso, il secondo bit sarà il numero 8, l'ultimo il numero 25.

Chiarito l'inizio e la fine, vediamo che cosa avviene in mezzo.

```
48 + 32 = 32
```

In mezzo ci sono sedici iterazioni, o round, di una serie di operazioni che parte da un blocco di 32 bit e uno di 48 bit per produrre un blocco di 32 bit. Il blocco di 32 bit arriva da metà del blocco di 64 bit risultante dalla permutazione IP iniziale. Chiamiamolo S. Chiamiamo D l'altra metà (Sinistra, Destra, ok?). Chiamiamo SD il blocco tutto intero. Chiamiamo S'D' il blocco che sarà il risultato di ogni round. I 48 bit arrivano dalla chiave e li chiamiamo B. Ogni round accade questo:

```
S' = D
D' = S(+)f(D,B)
```

SETTANTA MILIONI DI MILIARDI DI CHIAVI

È lo spazio-chiavi massimo teorico di DES. Tuttavia questo valore, nel computing di oggi, significa insicurezza. Il 17 luglio 1998 un computer da 220 mila dollari (DES Cracker, http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker) costruito dalla Electronic Frontier Foundation (EFF) ha violato DES in meno di cinque giorni con un attacco a forza bruta. Le specifiche ufficiali di DES possono essere lette a http://www.itl.nist.gov/fipspubs/fip46-2.htm.

dove (+) significa addizione bit per bit modulo 2 (1+0=1, 1+1=0)

La parte f(D,B) è più complessa

Sappiamo che D è una sequenza di 32 bit (metà del blocco iniziale di 64 bit). Lo facciamo diventare di 48 bit mescolando la sequenza e riproponendo due volte alcuni dei bit, secondo questo schema:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Il bit 1 dei trentadue ricorre due volte, una volta in seconda posizione e in ultima posizione. Eccetera. Questi 48 bit si incrociano con i 48 bit presi dalla chiave, nel passaggio più complicato di tutto il procedimento. Si eseguono otto funzioni che trattano un blocco da sei bit e restituiscono un blocco da quattro bit, secondo lo schema che segue (che è quello della prima funzione):

Riga	Colonna 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Il primo e l'ultimo bit del blocco di sei, in base 2, rappresentano un numero da zero a 3, che chiamiamo X. I quattro bit in mezzo invece rappresentano un numero da zero a 15, che chiamiamo Y. Guardiamo, come nella battaglia navale, all'incrocio della riga X e della colonna Y. Il risultato è un numero da 0 a 15, che è rappresentabile da quattro bit ed è l'output desiderato per il blocco di sei bit in ingresso. Per esempio, se il blocco di sei bit è 011011, la riga è 01 (cioè 1) e la colonna è 1101 (cioè 13). All'incrocio di riga 1 e colonna 13 sta il numero 5, che equivale a 0101. Ci sono altre sette funzioni identiche ma con schemi diversi, che si possono vedere alla pagina http://www.itl.nist.gov/fipspubs/fip46-2.htm.

Il blocco di 32 bit ottenuto dagli otto blocchi di quattro bit ciascuno viene sottoposto a una ulteriore permutazione secondo questo schema:

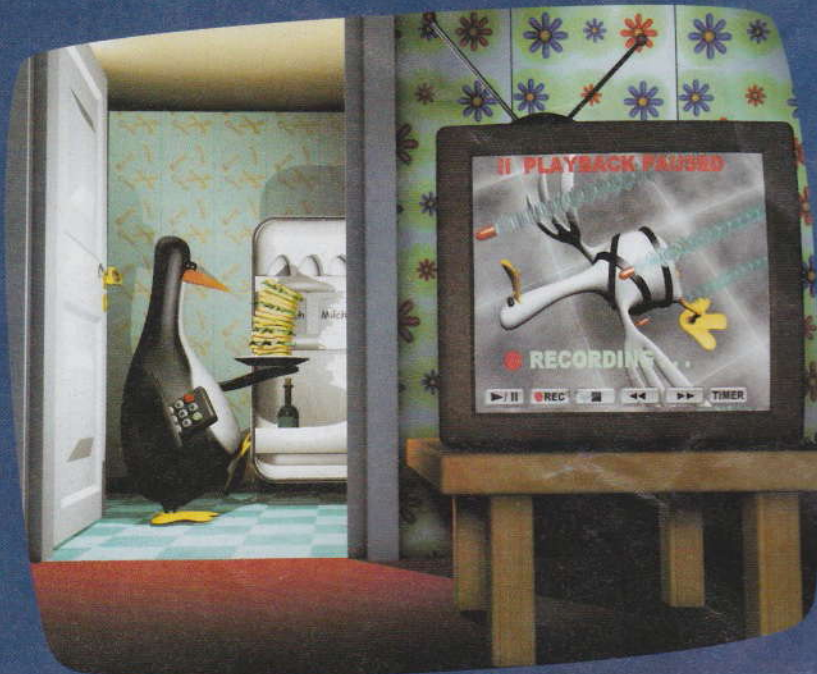
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Come già visto: il primo bit della nuova sequenza sarà il sedicesimo della vecchia; il secondo bit sarà il settimo; il terzo sarà il numero 20 e così via, fino al trentunesimo (penultimo, che sarà il vecchio numero quattro) e al trentaduesimo e ultimo, che sarà il venticinquesimo originale. Tutto il giro descritto, come detto, si verifica per sedici volte.

Prima di arrivare alla permutazione finale di cui abbiamo già parlato, la metà

destra e la metà sinistra del blocco di 64 bit vengono scambiate. Ed è tutto.

P. Greco
p.greco@hackerjournal.it

Linux visto da

C'è chi non abbandonerà mai Windows, ma un'occhiata a Linux gliela darebbe volentieri. Eccola!

Mio figlio ha quattordici anni e quest'estate ha lavorato come programmatore per pagarsi le vacanze. Ha imparato un po' di Python, MySQL, PHP e altro sw open source e non ha fatto altro che parlarmi di quanto è bello Linux.
Io uso Windows da quando esisteva la preistorica versione 3.1, però ho deciso di fare comunque una prova.

Non volevo modificare niente sul mio computer, che funziona bene, e così ho provato Knoppix, una versione gratis di Linux che parte direttamente da CD e non tocca assolutamente niente di quello che sta sul disco rigido. Dentro il CD c'è un sacco di software tra cui OpenOffice e Mozilla. Bisogna dire che il desktop ha un bell'aspetto, con le trasparenze e il pannello inferiore a scomparsa come il Dock di Mac OS X. Però Knoppix alla fine è una bella demo ed è difficile lavorarci in modo impegnativo per il computer.

Ho fatto una prova ulteriore sul computer di mio figlio, che ha installato Linux SUSE (http://www.suse.de/it) e lì ho sollecitato un po' OpenOffice (http://www.openoffice.org). In effetti sembra adeguato, anche se non ha niente di veramente par-

KNOPPIX LINUX INNOCUO E GRATUITO

Knoppix si può scaricare gratis e masterizzare su un CD. Dopo di che si può avviare il computer dal CD e usare Linux senza modificare neanche un bit di quello che sta sul disco rigido, e quindi provare Linux senza rischiare Windows. L'indirizzo generale di Knoppix è http://www.knoppix.net e si può scaricare direttamente da http://www.knoppix.net/get.php.

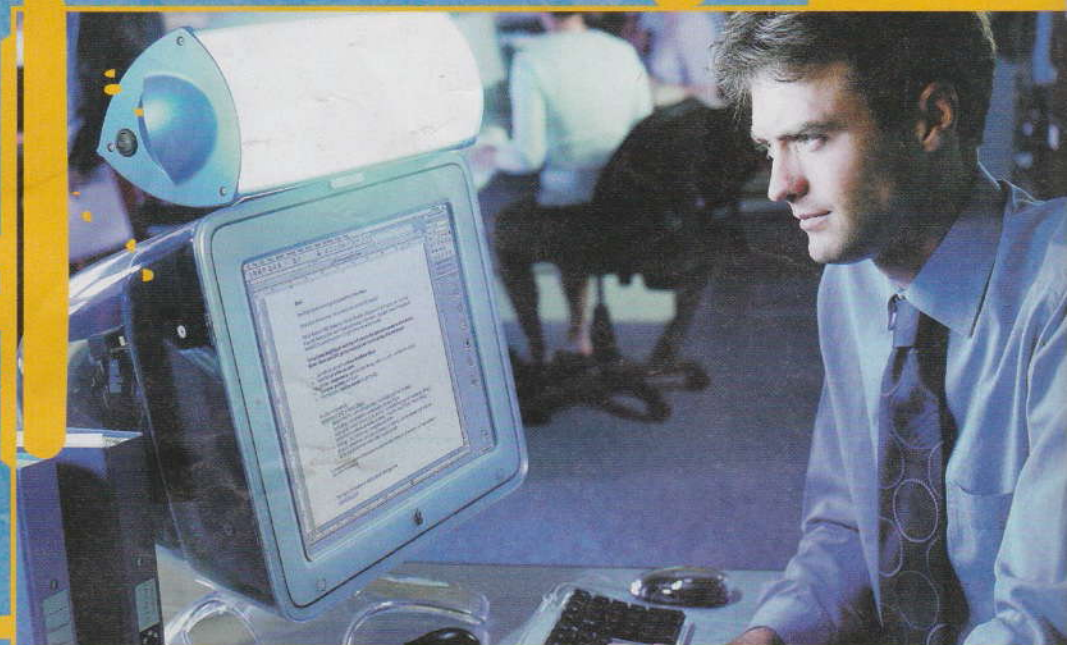
Windo$ws

ticolare rispetto a Office. Mozilla e Firefox sono browser sotto certi aspetti migliori di Explorer (soprattutto sono più sicuri) ma esistono anche per Windows e non rappresentano ragioni particolari per passare a Linux. Il desktop è amichevole, in italiano, molto configurabile e personalizzabile. Ma come provi ad aprire il cofano salta fuori subito Unix,

▲ *OpenOffice su Linux. Come si vede è praticamente come Word. La lingua? E' finlandese.*

un po' come in Windows salta fuori subito il DOS o ti ritrovi alle prese con il Registro.

Da vecchio appassionato a Windows, con più di dodici anni di abitudine, riconosco che Linux è un bel sistema. È più sicuro, è stabile, è gratuito, ci sono tanti programmi, è bello da vedere. Tutto sommato però non offre molto più di quello che offre Windows, se non per il fatto che è gratis. OpenOffice fa tutto quello che fa Microsoft Office, gratis, e questo è un argomento su cui non si discute. Ci sono tanti programmi, ma per Windows ce ne sono ancora di più. A livello desktop, secondo me la partita è pari. Si parlasse di server, beh, si sa che Linux è superiore. Ma sui desktop uno vale l'altro. È il mio parere, beninteso.

Karonte

Quale sarà il sistema più adatto per lavorare, giocare, divertirsi? Non c'è una risposta migliore delle altre. Windows è buono per tante cose, Linux pure, Mac OS X anche. L'importante è avere quello che si desidera e che il computer sia sicuro e affidabile!

BUONI E CATTIVI

Windows e Linux secondo il parere dell'autore. Il giudizio di ognuno di noi può cambiare, naturalmente, in funzione delle esperienze e dell'uso che vogliamo fare del computer.

	WINDOWS	LINUX
Installazione	Buono	Buono
Programmi	Buono	Buono
Sicurezza	Cattivo	Buono
Stabilità	Buono	Buono
Semplicità	Buono	Cattivo
Per lavorare	Buono	Buono
Per giocare	Buono	Cattivo
Prezzo	Cattivo	Buono

Domiamo il CENSORWARE

Liberi o sicuri? Forse i termini del problema non sono esattamente questi. Comunque i programmi che limitano la navigazione sono inutili. Ecco perché...

IL TRUCCO PIÚ SEGRETO

Anche NetNanny pare abbia una backdoor, lasciata lì dai programmatori. Proviamo a usare la password "~frontdoor" (virgolette escluse). A volte funziona.

Sentendo parlare di NetNanny ci viene un po' da ridere. Oltre che avere un nome del tutto infantile, lui e i suoi simili sarebbero nati per evitare di cascare nei siti considerati inopportuni o offensivi. Ma è proprio così? In realtà non esiste un metodo tecnicamente sicuro per evitare di cadere dentro le diverse piovre delle schifezze umane: anzi, oltre al danno della censura imperfetta i programmini in questione portano con sé anche la beffa di limitare alla grande la libertà di navigare. Bloccando, per esempio, anche siti dove di tumore al seno (ahi!) si parla in modo semplice ed esplicitamente chiaro, oppure dove viene spiegata la trasmissione tramite rapporti sessuali (ahi!) dell'Aids, e così via. Vi ricordate ad esempio l'articolo in cui abbiamo raccontato che L'Internet Security di Symantec blocca l'accesso al sito di HJ perché lo ritiene pericoloso? Se ci pensiamo bene, non poter usare alcuni termini – perché su questo si basano la maggior parte dei programmi in questione – è di per sé un enorme limite alla disponibilità di informazioni, in un mondo in cui tutto accade e tutto può accadere, da qualche parte. E tutto viene ormai regolarmente e spesso proficuamente registrato sulla rete, da qualche parte. Ok, allora vediamo come liberarci da questa inutile censura.

Come liberarci da NetNanny

La versione 4.0 la eliminiamo da Start > Esegui. Scriviamo msconfig facendo partire l'Utilità di configurazione del sistema. Andiamo su Avvio e togliamo la spunta da "nntray.exe" e "NNSvsc", poi riavviamo. Fatto. Oppure disabilitiamolo al momento direttamente dal task manager (Ctrl-Alt-Delete). Troviamo il task OCRAWARE o Wnldr32 (dipende dalla versione) e un clic su Termina operazione sarà sufficiente. Per eliminarlo proprio del tutto, cerchiamo il file c:\windows\system.ini.
Facciamone una copia di sicurezza con un altro nome, che terremo. Non si sa mai. Apriamolo con Blocco note e cerchiamo l'intestazione [boot]. Lì sotto dovrebbe esserci qualcosa come drivers= seguito da una lista, tra cui wndrv16.dll. Cancelliamolo (solo quello!). Salviamo il file e il gioco è fatto.

Se vogliamo ripulire il campo anche dal file di log, cerchiamo e cancelliamo Wnn3.log nella directory di Net Nanny. Il file è cifrato, quindi lo si deve eliminare in blocco, non lo si può modificare.

Con SurfWatch si fa così

Per i più esperti e per tutti quelli che non hanno paura di toccare i registri di sistema, ecco come si fa. Apriamo la cartella di Avvio ed eliminiamo il collegamento a SurfWatch e quello a SurfWatch Updater.
Apriamo il file win.ini e cambiamo la linea

```
load= C:\CO_RO_NT\surfctl.exe
```

lasciando solamente

```
load=
```

Andiamo su Start > Esegui > regedit e cancelliamo la chiave GraphicsFilter, che è una sottochiave di

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
```

Il valore di questa chiave sarà

```
C:\CO_RO_NT\surfctl.exe.
```

Eliminiamola.

Riavviamo il computer in modo DOS (F8 al riavvio).
Spostiamoci nella cartella c:\windows\system\ directory e scriviamo:

```
attrib -h -r -s system.drv
attrib -h -r -s net.drv
move system.drv system.bak
move net.drv system.drv
```

Scriviamo win per riavviare Windows. Se appare qualcosa come: Windows sta eseguendo uno o più programmi MSDOS... scriviamo semplicemente exit. SurfWatch sarà ora disabilitato. Se rifacciamo i passaggi all'inverso lo possiamo recuperare.

One4Bus
one4bus@hackerjournal.it

Così com'è al momento dell'installazione PHP funziona perfettamente ma, se vogliamo veramente usarlo al massimo, dobbiamo aprirne il cofano!

i SEGRETI del file

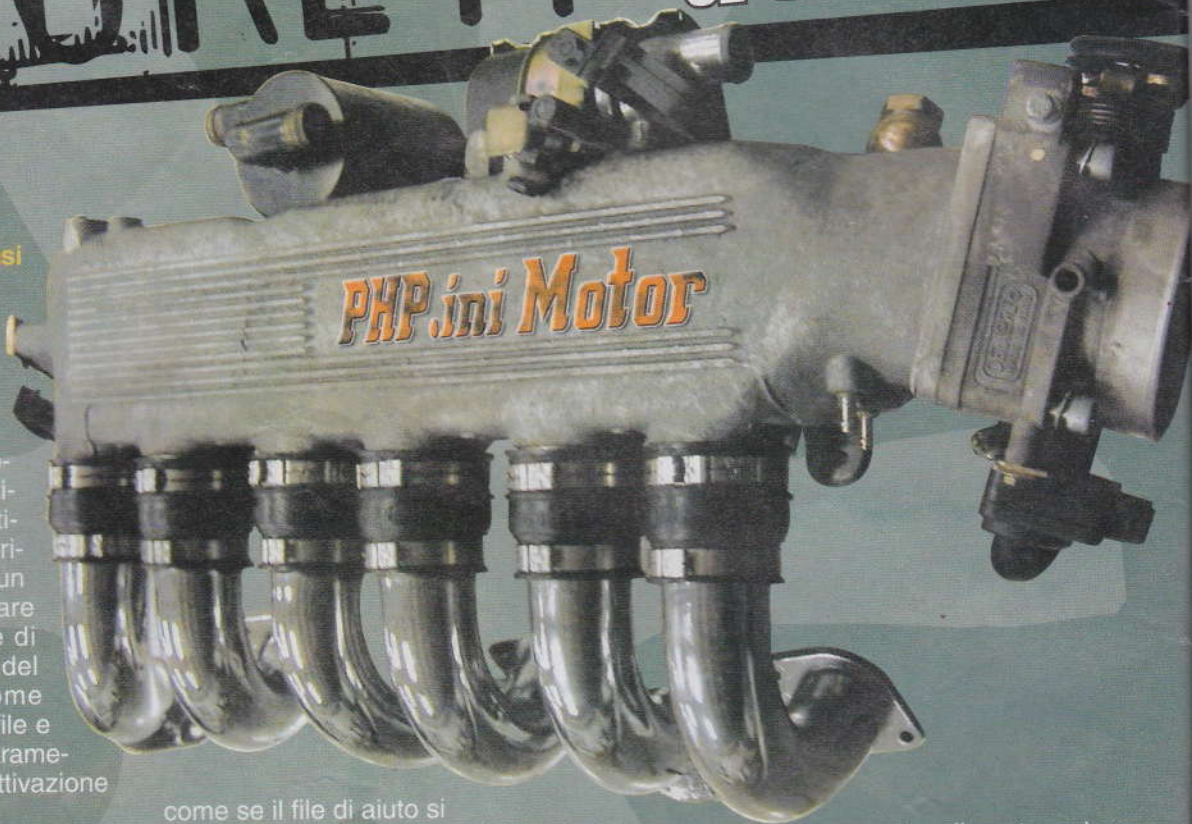
PHP.ini Motor

Php può essere, quasi sempre, installato con le preimpostazioni di serie. Funziona e funziona bene. Ma i programmatori di PHP sanno che molti hanno voglia o bisogno di configurazioni alternative da usare in situazioni particolari e per questo hanno inserito una serie di variabili dentro un file di nome php.ini. Smanettare dentro questo file permette di modificare numerosi aspetti del comportamento di PHP, come impostazione dei percorsi di file e directory, cambiamento dei parametri di sessione e database e attivazione o meno di estensioni.

Un tranquillo file di configurazione

La struttura di php.ini è identica a quella di altri file .ini che si trovano in Windows, Linux e Mac OS X: un file ASCII diviso in sezioni, ognuna delle quali contiene le variabili relative a quella sezione. Un file php.ini tipico è come composto da tanti mattoni del tipo

```
[Sezione]
variabile="valore"
altravariabile="altrovalore"
```

con un bel po' di commenti in mezzo, come se il file di aiuto si fosse mescolato ai comandi (e un po' è proprio così).

Ogni variabile e il suo valore stanno da soli su una riga; il nome della sezione è tra parentesi quadre e se una riga inizia con il punto e virgola (;) è un commento. I valori delle variabili distinguono tra maiuscolo e minuscolo e possono essere numerici (123…), stringhe (abc…) o booleani (true, false).

Primo trucco utile: approfittare dei commenti. Quando modifichiamo una variabile, invece di cancellare il vecchio valore lo commentiamo e inseriamo una nuova riga, con la stessa variabile e il valore modificato.

Così il vecchio valore resta inattivo, ma a disposizione, e se in seguito vogliamo cambiarlo di nuovo è sufficiente spostare il punto e virgola da una riga a un'altra.

Il file deve per forza trovarsi dove PHP è in grado di accorgersi che c'è. Deve essere la directory di lavoro corrente, oppure la directory inserita nella variabile ambientale $PHPRC oppure quella specificata al momento della compilazione. Nel caso di Windows, quest'ultima corrisponde alla directory principale di Windows.

Se usiamo PHP attraverso il server Web, dovremo riavviare il server prima di vedere in atto le modifiche alla configurazione. Se lo usiamo da riga di comando invece il file di configurazione verrà letto appena richiamiamo il binario di PHP.

PHP.ini

I sito di riferimento per sapere tutto quello che serve su PHP è, chiaramente, http://www.php.net. Da vedere soprattutto la sezione Documentation, che è completissima. Per risorse e istruzioni in italiano, cercare http://www.latoserver.it/php/pi-accapi.php3 e http://www.phpitalia.com.

Opzioni di parsing

Sono le variabili che determinano il funzionamento dell'interprete PHP.

Engine = On

Significa che il server Web interpreta il codice PHP quando lo trova in una pagina. Ha senso che sia così e va lasciato su On, ma qualcuno potrebbe voler disabilitare momentaneamente l'interpretazione per qualche motivo e, allora, cambierebbe il valore in Off.

short_open_tag = On

Decide se vengono riconosciuti o meno i tag abbreviati di PHP, <?… ?> oppure solo quelli standard, <?php… ?>. Utile nel caso di conflitti con altri linguaggi o di pagine HTML particolarmente rigorose nella stesura del codice.

output_buffering = Off
output_buffering = 1024

Di solito i dati di sessione, cookie e header HTTP in uno script PHP devono essere inviati prima della generazione di qualsiasi output. Se questo non è possibile si può abilitare l'output buffering di PHP, mettendo questa variabile a On. Alternativamente il valore della variabile può essere un numero, che indica le dimensioni del buffer.

expose_php = On

Questa variabile decide se all'avvio di PHP il server Web riceverà o meno il numero di versione del linguaggio. Mettendo la variabile a Off questo non accade. Può essere utile, per esempio, per mascherare la configurazione del server Web allo scopo di rendere più difficile un attacco al server stesso.

In un prossimo articolo torneremo sul tema e affronteremo altri pezzi di php.ini, tra cui la gestione degli errori, per poi passare ad argomenti ancora più tosti.

Nel frattempo, iniziamo a guardarci il file e a cercare di capire che funzioni svolgono le varie variabili, anche aiutandoci con i commenti. A presto!

Nyarlathotep
nyarlathotep@hackerjournal.it

STRINGHE E COMMENTI

L'inizio di un classico file php.ini. Le righe che iniziano con un punto e virgola sono commenti.

```
[PHP]

;;;;;;;;;;;
; WARNING ;
;;;;;;;;;;;
; This is the default settings file for new PHP installations.
; By default, PHP installs itself with a configuration suitable for
; development purposes, and *NOT* for production purposes.
; For several security-oriented considerations that should be taken
; before going online with your site, please consult php.ini-recommended and
; http://php.net/manual/en/security.php.


;;;;;;;;;;;;;;;;;;;
; About this file ;
;;;;;;;;;;;;;;;;;;;
; This file controls many aspects of PHP's behavior.  In order for PHP to
; read it, it must be named 'php.ini'.  PHP looks for it in the current
; working directory, in the path designated by the environment variable
; PHPRC, and in the path that was defined in compile time (in that order).
; Under Windows, the compile-time path is the Windows directory.  The
; path in which the php.ini file is looked for can be overridden using
; the -c argument in command line mode.
;
; The syntax of the file is extremely simple.  Whitespace and Lines
; beginning with a semicolon are silently ignored (as you probably guessed).
; Section headers (e.g. [Foo]) are also silently ignored, even though
; they might mean something in the future.
;
; Directives are specified using the following syntax:
; directive = value
; Directive names are *case sensitive* - foo=bar is different from FOO=bar.
;
; The value can be a string, a number, a PHP constant (e.g. E_ALL or M_PI), one
; of the INI constants (On, Off, True, False, Yes, No and None) or an expression
; (e.g. E_ALL & ~E_NOTICE), or a quoted string ("foo").
;
; Expressions in the INI file are limited to bitwise operators and parentheses:
; |        bitwise OR
; &        bitwise AND
; ~        bitwise NOT
; !        boolean NOT
;
; Boolean flags can be turned on using the values 1, On, True or Yes.
; They can be turned off using the values 0, Off, False or No.
;
```

GERARDO SERINO
338342557/064067171

Magico

Qualche anno fa, nella preistoria di Internet, dire dove si trovavano i computer su una rete era un gioco da ragazzi. Oggi è un sistema che ha del magico

IL CREATORE DEL DNS

Paul Mockapetris inventò il DNS nel 1984 per risolvere il problema della crescita dei nomi su Internet. Prima esisteva solamente un file, conosciuto come tabella degli host, mantenuto presso lo Stanford Research Institute's Network Information Center (SRI-NIC). Un paio di volte alla settimana questo istituto aggiornava la tabella con i nuovi nomi. Gli amministratori delle reti collegate recuperavano la tabella via FTP e tutti erano felici e contenti, almeno per un po'.
L'idea geniale del sistema di Mockapetris, il DNS, è stata quella di liberare il sistema dal controllo di una singola organizzazione, costruendo quello che ora chiamiamo un database distribuito, in tutto il mondo.

▲*Paul Mockapetris: ha inventato lui il database distribuito dei DNS.*

Il sistema che organizza i nomi che troviamo su Internet: questo è il DNS. Solamente che detto così può apparire un giochetto da quattro soldi, ma se ci pensiamo bene è... qualcosa di folle, di universale, che sa di onnipotenza. Pensiamo a quanti nomi di dominio esistono al mondo. Sappiamo che tutto è associato ai numeri degli indirizzi IP. Pensare che ci siano dei sistemi che riescono a tradurre miliardi di nomi in numeri precisi e che lo fanno in una manciata di microsecondi è qualcosa che ricorda l'osservazione del cielo stellato. La stessa sensazione di meravigliosa impotenza. Eppure gli amministratori di sistema devono porsi la domanda praticamente ogni giorno: è tutto a posto sul nostro DNS?

DNS è...

Il sistema DNS consiste di tre componenti: i dati (chiamati record delle risorse), i server (chiamati server dei nomi di dominio), e i protocolli Internet che comunicano i dati tra i server.
I miliardi di record delle risorse nei DNS sono suddivisi in milioni di file chiamati zone. Le zone sono memorizzate su alcuni server specializzati ("autoritari") distribuiti un po' dappertutto, i quali rispondono alle richieste sulla base dei record delle risorse nelle zone di cui loro sono a conoscenza.
I server cache sono invece quelli che chiedono ad altri server le informazioni e quindi le memorizzano temporaneamente. Un server può essere un server autoritario per una zona e fungere da server cache per le altre interrogazioni. Alcuni server autoritari lo sono perché mantengono i dati di decine o centinaia di zone, ma generalmente i server hanno autorità solo per poche zone vicine.
Il tutto vuole in pratica dire, per esempio, che www.qualchedominio.com corrisponde a qualcosa come 208.178.167.7 (non è vero, è solo un esempio!). Per saperlo, un client come il nostro browser o come il client di posta invia una richiesta di un record al server DNS. Il record è

DNS

◄ *La magia si svela se ci rivolgiamo a www.dnsstuff.com. Più che magico: efficientissimo!*

appunto l'indirizzo IP corrispondente al nome ed è conosciuto come record A. Il nome può anche essere un alias di un record A differente (per esempio www.qualchedominio.com può essere un alias di un nome come server01.qualche-dominio.com),: in tal caso viene chiamato CNAME. Quando chiediamo al nostro DNS locale un record che non è presente, si scatena la caccia sui DNS intorno fino a trovare la risposta. Questa viene poi messa nella cache locale per usi immediatamente successivi.

DNS in azione

Possiamo facilmente vedere il nostro DNS in azione eseguendo il comando Nslookup in Start > Esegui

Ancora meglio, possiamo sfruttare un servizio on line che troviamo all'indirizzo http://www.dnsstuff.com/

Cerchiamo la funzione DNSLookup (in alto a destra) e inseriamo il nome di dominio che vogliamo osservare.

Possiamo perfino scegliere il campo da visualizzare del data base del DNS.

Il risultato è completo e ci dà un sacco di informazioni anche su tutti i DNS che sono stati interrogati per arrivare al dominio richiesto.

ControlBus
controlbus@softhome.net

▲ *Il risultato di un'interrogazione: il percorso dei DNS, interrogati in tempo reale. Nessuna cache di mezzo.*

INSTALLIAMO UN DNS?

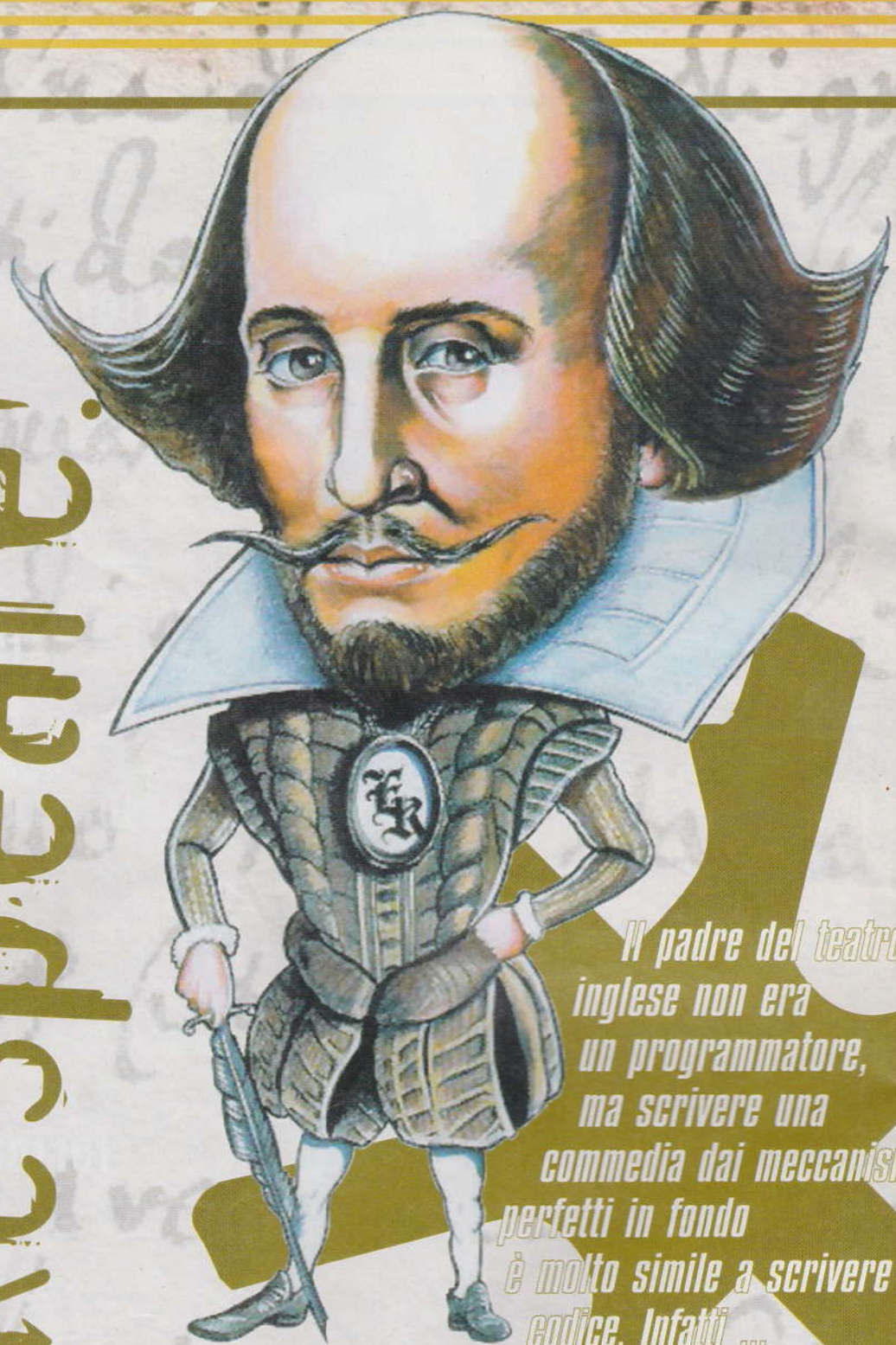
▲ *Qualcuno ci ha pensato, e a sviluppato un'interfaccia grafica per il server DNS più diffuso al mondo.*

Se abbiamo un server da gestire, ne siamo amministratori. Come tutti gli amministratori, sappiamo che DNS non è una bestia tanto semplice da domare. Sicuramente è uno dei servizi più importanti che dobbiamo mettere sul nostro server.

Siccome siamo quasi sicuramente nella grande maggioranza dei fortunati amministratori di server Unix (o Linux), utilizzeremo il più diffuso sistema di DNS esistente: BIND (Berkeley Internet Name Domain).

Prima d'ogni altra cosa lo scarichiamo da www.isc.org, l'organizzazione no-profit che l'organizza. Mentre scriviamo, la versione più recente è la ISC BIND 9.3.0rc4.

Purtroppo per noi, però, configurare BIND non è sempre un gioco da ragazzi e quindi il consiglio è procurarci quanto prima l'interfaccia grafica di configurazione appositamente sviluppata per BIND. La troviamo all'indirizzo www.lysator.liu.se/~backstrom/kcmbind/

Programmiamo come faceva Shakespeare!

Il padre del teatro inglese non era un programmatore, ma scrivere una commedia dai meccanismi perfetti in fondo è molto simile a scrivere codice. Infatti ...

Sapete cosa hanno fatto due studenti scandinavi alle prese con uno stupido lavoro di analisi da portare al corso di programmazione? Hanno inventato un linguaggio di programmazione tutto loro che si rifà alle opere del famoso drammaturgo inglese: lo Shakespeare Programming Language, SPL.

Di linguaggi buffi ne esistono, ma questo li batte tutti, perché la sua struttura dà al

CARTA D'IDENTITÀ DELLO SPL

Nome: Shakespeare Programming Language
Nato nel: febbraio 2001
Genitori: Karl Hasselström e Jon Åslund
Indirizzo: http://shakespearelang.sourceforge.net/report/shakespeare/
Segni particolari: si converte direttamente in C istruzione per istruzione e combina, dicono ironicamente i genitori, l'espressività del BASIC con l'amichevolezza del linguaggio assembly.

codice l'aspetto di un'opera teatrale di Shakespeare, I personaggi entrano ed escono di scena, si parlano, l'opera procede di atto in atto e tutto conserva una coerenza interna ammirevole, tanto è vero che ogni singola battuta, ehm, istruzione in SPL può essere convertita nel più convenzionale linguaggio C.

Lo Shakespeare Programming Language non è particolarmente sofisticato; le sue strutture interne si limitano ad aritmetica di base e istruzioni di salto (goto). Ma ci si può fare ugualmente molto. La prima parte di un programma SPL è il titolo. Può essere lungo a piacere. In pratica il primo paragrafo di un programma SPL fa da titolo. Poi vengono introdotti i personaggi. Ognuno di essi in realtà è il corrispondente di una variabile, ognuna in grado di contenere un valore intero. Attenzione, però: anche se la descrizione che segue il loro nome può essere di fantasia, i nomi devono essere quelli di veri personaggi shakespeariani, come Romeo, Juliet o persino il Ghost (il padre assassinato di Amleto).

171 BYTE

Lo Shakespeare Programming Language è affascinante ma produce codice ingombrante. Per disintossicarsi non c'è niente di meglio che Brainfuck: un linguaggio nato per avere il compilatore più piccolo possibile. C'è chi è riuscito ad arrivare a 171 byte! Tutte le notizie del caso si trovano a http://www.muppetlabs. com/~breadbox/bf.

Il programma viene diviso in atti e gli atti sono suddivisi in scene, proprio come in una commedia. Ma agli effetti della programmazione queste sono subroutine e saltare da un atto o da un altro atto (o scena) ha l'effetto di un goto. I personaggi entrano, proprio come sul palco, pronunciano le loro battute, escono, eccetera. Leggendo codice SPL sembra che da un momento all'altro possa calare il sipario. Invece il gioco può continuare a lungo, dato che il linguaggio funziona davvero.

Kurt Gödel
kurtgoedel@hackerjournal.it

FATTORIALIZZARE O NON FATTORIALIZZARE, QUESTO IL PROBLEMA

Nel lontano Hacker Journal 53 il cyberenigma proponeva di indovinare che cosa facesse una funzione scritta in più linguaggi di programmazione: Ai più bravi veniva proposto di riscrivere la stessa funzione in un linguaggio diverso da quelli presentati. La funzione era quella di fattoriale (il fattoriale di 6 si scrive 6! e significa 1 * 2 * 3 * 4 * 5 * 6 = 720). Infernet89 ci ha inviato la funzione di fattoriale scritta in Shakespeare Programming Language (http://shakespearelang.sourceforge.net/report/shakespeare/): come si vede, programmare non è tanto diverso dal fare teatro!

SHAKESPEARE

```
[enter Hamlet and Romeo]
Hamlet:
You are a sum of an hero and thiself!
Open your hearth!
Romeo:
You lying stupid big smelly coward!
You are a sum of a big knife and thiself!
Speak your mind!
[enter Hamlet and Otello]
Hamlet:
You are a difference from Romeo and a flower!
You are the product of Romeo and thiself!
Open your hearth!
[enter Juliet and Hamlet]
Hamlet:
You are a small red flower!
Romeo:
Am i nicer than you?
Juliet:
If so, let's proceed to Scene IIII
Juliet:
Am i nicer than you?
Romeo:
If so, let's return to Scene I
[enter Romeo and Giulietta]
Giulietta:
Open your earth!
```

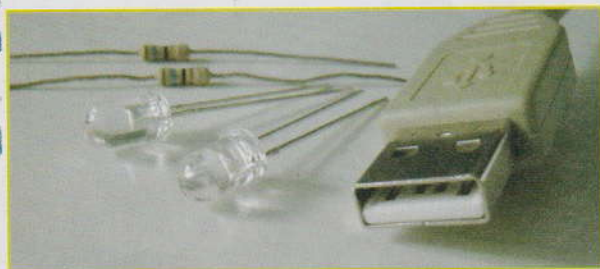
SPL non è l'unico modo in cui Shakespeare attira i programmatori. :-)

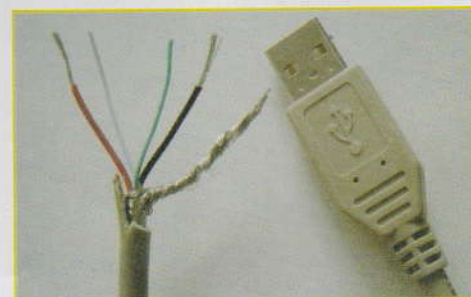
HACKING di

Spesso basta un po' di fantasia e qualche semplice componente per ottenere risultati di grande soddisfazione.

Ecco cosa possiamo fare con un cavo Usb e un paio di Led

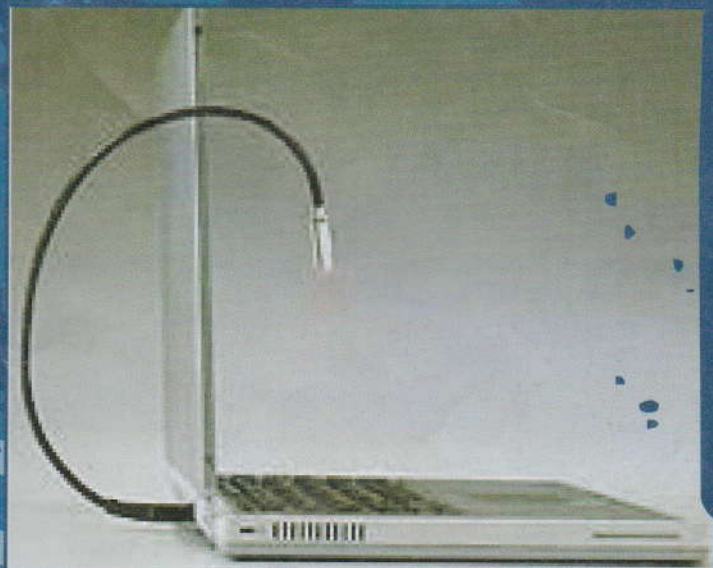
IL MONTAGGIO

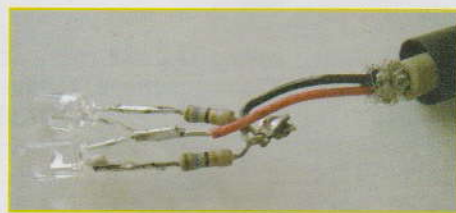
CONTINUA A PAG. 28

Questi sono i componenti necessari. Del cavo Usb dobbiamo salvare la spina piatta che si inserisce nel pc. L'altro capo del filo può avere qualunque tipo di terminazione perché non ci interessa: la taglieremo e la butteremo via. Quindi massima attenzione a non sbagliarsi: abbiamo bisogno di un po' di cavo attaccato a questa spina.

Tagliamo il cavo Usb e con attenzione togliamo circa due centimetri di guaina. Spostiamo la calza metallica e lo schermo metallico e vedremo apparire quattro fili. Uno bianco e uno verde, in genere più sottili, e uno rosso e uno nero, che sono quelli dell'alimentazione e ci interessano. In genere sono anche leggermente più spessi.

un cavo USB

Lo scopo è quello di costruire una luce molto brillante a spot, da visione notturna, direttamente collegabile alla porta Usb del nostro pc. Molto utile se abbiamo un notebook e ci troviamo in una situazione di buio assoluto, o se dobbiamo utilizzarlo di sera senza dare fastidio a chi ci sta accanto. Attaccata a un pc desktop e con un cavo sufficientemente lungo, ce ne sono anche di tre metri e oltre, è un utilissimo accessorio per illuminare con precisione e chiaramente zone inaccessibili dentro il nostro pc, mentre lo controlliamo, cambiamo schede, spostiamo switch o altro.

Il materiale da procurarci

Una cavo Usb qualunque, che andrà tagliato. Quindi scegliamolo il più economico possibile. Costo approssimativo: circa due euro e lo troviamo negli ipermercati o nei negozi di computer. Due Led bianchi ad alta luminosità. Naturalmente possiamo sceglierli anche colorati, per dare alla luce effetti speciali. Ma se ci serve una luce che illumini veramente, scegliamoli bianchi. Questi componenti costano un po': noi li abbiamo pagati 2,75 euro ciascuno, ma ne vale la pena. Li possiamo trovare presso un negozio di componentistica elettronica, oppure su diversi siti (per esempio www.rk-elettronica.it o altri).
Due resistenze da 56 ohm (ma anche da 47 ohm vanno bene).
Inoltre ci può servire un pezzetto di guaina termorestringente, utile per tener fermi i Led e rendere maneggevole il tutto.

Tagliamo senza pietà sia la calza metallica che i fili bianco e verde. Teniamo e speliamo i fili rosso, il polo positivo dell'alimentazione, e nero, il polo negativo. Infiliamo nel cavo circa cinque centimetri di guaina termorestringente. Ci servirà per bloccare il tutto, ma non è indispensabile: se vogliamo otteniamo lo stesso scopo con qualche giro di nastro isolante o con un nastro autoagglomerante (lo si trova da un ferramenta).

Il principio di collegamento è questo: in serie, si saldano ai fili dell'alimentazione

la resistenza da 56 ohm e il diodo Led. La resistenza può essere messa o sul filo rosso o su quello nero, ma per il Led va rispettata la polarità. Il terminale più corto del Led è il catodo ed è segnalato anche da una tacca sul corpo del Led stesso. Il catodo va collegato con il filo nero (-). Il terminale più lungo è l'anodo e va collegato con il filo rosso (+).

Isoliamo molto bene i singoli fili scoperti con dei piccoli pezzi di nastro isolante. Non devono assolutamente toccarsi, pena la distruzione della porta Usb del nostro computer per cortocircuito!

Tiriamo la guaina termoisolante fino a coprire i Led, lasciandone ovviamente scoperta la punta. Con un phon per capelli, tenuto mol-

Ovviamente ci serve anche un saldatore, un po' di stagno, un tronchesino o una forbice per spelare i fili. Ovvero quella attrezzatura minima che ogni buon hacker dovrebbe avere.

Cosa sfruttiamo

Usiamo la tensione presente sull'alimentazione della porta Usb per accendere i due diodi Led messi in parallelo. Ovviamente dobbiamo stare attenti a non assorbire troppa corrente per non rovinare la porta e a fare le cose con precisione per non creare mai dei cortocircuiti che metterebbero fuori uso la porta Usb del nostro computer.

Una luce per porta USB costa intorno ai 15 euro, noi ne abbiamo spesi meno di 8, ma vogliamo mettere la soddisfazione di aver fatto da soli

Usb senza segreti

Agli estremi della presa Usb si trova l'alimentazione, ovvero una tensione di 5 Volt, per nulla pericolosa, che è possibile caricare al massimo con 500 mA. (milliampere = millesimi di ampere). Se andiamo oltre, sul pc appare un messaggio del driver che ci dice che la periferica non funziona per troppo assorbimento. Ecco perché si usano gli hub Usb autoalimentati. Quando le periferiche diventano troppe, oppure qualcuna ha bisogno di più corrente, bisogna per forza aggiungere un alimentatore esterno che fornisca tutta la corrente necessaria.
Non è il caso della nostra luce a Led. Un Led assorbe, infatti, dai 10 ai 20 mA e quindi, mettendone un paio, arriviamo al massimo a un decimo della corrente prelevabile. Niente di preoccupante.

Il montaggio

CONTINUA DA PAG. 27

to vicino, scaldiamo la guaina, che diventa un tutt'uno con il filo e il corpo dei Led.
Così abbiamo creato una luce maneggevole e protetta.

Attacchiamo il cavo alla porta Usb e se abbiamo fatto tutto con attenzione funziona al primo colpo: abbiamo la nostra luce spot e ci meraviglieremo di com'è luminoso questo tipo di Led.

Anche nel buio più assoluto avremo una luce autonoma più che sufficiente per illuminare la tastiera senza disturbare nessun altro che possiamo avere intorno.
Teniamo il nostro cavo-luce sempre in borsa: come luce di emergenza è assolutamente ideale in mille situazioni!

ENCICLOPEDIA dell'Hacking!

SQLInjection

SQLINJECTION È UNA TECNICA D'ATTACCO ALLE APPLICAZIONI WEB CHE UTILIZZA DELLE INTERROGAZIONI SQL (STANDARD QUERY LANGUAGE, IL LINGUAGGIO STANDARD DI INTERROGAZIONE DI MOLTI SISTEMI DI DATA BASE) IMMESSE DIRETTAMENTE DAL CLIENT. L'IDEA DI BASE CHE STA DIETRO ALLA TECNICA SQLINJECTION È QUELLA DI MANIPOLARE I DATI PASSATI ALL'APPLICAZIONE WEB IN MODO DA MODIFICARE OPPORTUNAMENTE L'INTERROGAZIONE AL DATA-BASE SUL SERVER, COSÌ DA OTTENERE DELLE RISPOSTE NON PREVISTE NEL PROGETTO WEB ORIGINALE.

ESEMPIO

Supponiamo di voler manipolare una tabella di dati, a partire da una pagina Html che comunica al data base, tramite uno script Asp, di fare il controllo dell'esistenza dell'utente. La pagina di login chiede semplicemente username e password.
Il codice Asp che consente questo potrebbe essere simile al seguente:

```
username = Request.form("username");
password = Request.form("password");
var rso = Server.CreateObject("ADODB.Recordset");
var sql = "select * from users where username + '" +
username +
"' and password = '" + password + "'";
rso.open( sql, cn );
```

Se ci chiamiamo 'sesamo' e usiamo la password 'apriti' normalmente l'interrogazione al data base sarà:

```
select * from users where username = 'sesamo' and
password = 'apriti'
```

Se però scriviamo

```
Username: se'samo
Password: apriti
```

la query al database diventa

```
select * from users where username = 'se'samo' and
password = 'apriti'
```

che restituisce un errore simile a questo:

```
Microsoft OLE DB Provider for ODBC Drivers error
'80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Line
1: Incorrect
syntax near 'samo'
/process_login.asp, line 46
```

che ci dice che una virgoletta ha fatto terminare la lettura dello username e quindi il resto è qualcosa che il database non capisce.
Questo ci suggerisce che se scriviamo solamente

```
Username: ' or 1=1- -
```

(occhio alle virgolette) prova nella pagina di Simone login utente.

il tutto funziona perché la query diventa

```
select * from users where username = '' or 1=1--' and
password = ''
```

e siccome i due trattini - - per Sql significano che da lì in poi è un commento e non tiene conto di ciò che c'è scritto, con un'interrogazione così otteniamo tutta la tabella degli 'user' registrati nel data base, perché qualunque espressione in OR con un'espressione sempre vera (1=1) è per forza sempre vera. Inoltre ci ritroviamo registrati automaticamente perché il sistema prende il primo nome della tabella e lo usa come utente corrente.

Sfruttando altri comandi di Sql sarebbe possibile a questo punto anche inserire dei nuovi utenti, cambiare o cancellare la tabella password e così via.

Cosa serve conoscere

Serve conoscere come funzionano i data base collegati ad applicazioni web, e in questo senso un'occhiata a http://www.extropia.com/tutorials/sql/toc.html potrebbe esserci d'aiuto.
Serve un po' di conoscenza delle istruzioni Sql: ne troviamo anche a questo link http://www.w3schools.com/

Security

Non esiste un metodo di difesa unico e totalmente sicuro, ma si possono adottare accorgimenti innanzitutto sul database, così che per esempio non risponda con log di errore, non consenta l'inserimento di commenti, non accetti codici diversi, sia messo dietro sistemi di autenticazione differenti e così via. Dei controlli potrebbero usare delle espressioni regolari che verifichino che le stringhe immesse o i dati immessi rientrino sempre dentro un range di parametri prefissato.

PER SAPERNE DI PIÙ: http://www.imperva.com/application_defense_center/white_papers/blind_sql_server_injection.html#overview

ENCICLOPEDIA dell'Hacking!

Firewall

"Porta antincendio", nella sua traduzione più logica in italiano, che consente di sezionare due o più parti di una rete. Per esempio può dividere la rete Internet dalla rete locale. Si distinguono due tipi principali di firewall: i packet type e gli application type. I primi smontano e controllano le intestazioni dei pacchetti TCP/IP in transito e quindi ne analizzano il contenuto, mentre i secondi cercano di capire cosa contengono i dati e lavorano su quelli. Nella pratica con i primi si possono prevenire attacchi dall'esterno, perché si analizza che tipologia di pacchetti sta arrivando. Con i secondi, gli application type, si possono fermare dei virus o altre applicazioni malefiche.

ESEMPIO

Il firewall si piazza tra l'esterno e la rete che vogliamo proteggere. Meglio se dedichiamo una macchina alla sola funzione di firewall, così che contenga solamente il sistema operativo e il software che agisce da firewall. Il S.O. migliore per questo scopo è attualmente Linux, perlomeno perché
- è gratuito
- consente protezioni a livello di pacchetto IP e di applicativo
- è possibile applicare la funzione di masquerading,
ovvero di non fare vedere all'esterno gli indirizzi delle macchine nella rete protetta
- è possibile metterlo su macchine anche obsolete e quindi abbattere i costi.

I modi di protezione che generalmente si adottano sono ipchains o iptable a livello del kernel e i tcp_wrapper a livello applicativo. A livello di kernel la protezione è più sicura, anche se la configurazione è piuttosto complessa.
Le regole di protezione sono scritte in un file di testo che viene letto sequenzialmente, ma viene applicata una regola solo la prima volta che la si incontra.
Questo significa che a fronte di due regole contrapposte nel file, viene applicata solo la prima incontrata. La forma di un file di regole è simile alla seguente, che riporta solamente un pezzo di file possibile:

```
[..............]
#############################################################
#INPUT RULES                                                #
#############################################################
#-----------------------------------------------------------#
# Incoming traffic on internal LAN                          #
#-----------------------------------------------------------#

# Allow everything on our LAN
#-----------------------
iptables -A INPUT -j ACCEPT -i $INTIF
iptables -A INPUT -j ACCEPT -i $CIPE
iptables -A INPUT -j ACCEPT -i lo  # Somewhat redundant,
but leave it.

#-----------------------------------------------------------#
# Incoming traffic on Internet interface                    #
#-----------------------------------------------------------#

# Add any real IPs behind the gateway here
#----------------------------------

# Block IPs that should never show up on our Internet
interface
#-----------------------------------------------------
iptables -A INPUT -j drop-reserved -i $EXTIF -s 127.0.0.0/8
iptables -A INPUT -j drop-reserved -i $EXTIF -s 1.0.0.0/8
iptables -A INPUT -j drop-reserved -i $EXTIF -s 23.0.0.0/8
iptables -A INPUT -j drop-reserved -i $EXTIF -s 31.0.0.0/8
iptables -A INPUT -j drop-reserved -i $EXTIF -s 96.0.0.0/3
iptables -A INPUT -j drop-reserved -i $EXTIF -s 128.0.0.0/16
[..............]
```

Cosa serve conoscere

La configurazione di un sistema Linux. Un buon punto di partenza: www.ziobudda.net

La sintassi delle regole e':

- **-A - Append**, aggiungiamo la regola alla precedente
- **-D - Delete**, cancella la regola indicata
- **-L - mostra** la lista delle regole
- **-F - Flush**, butta le regole a una a una
- **-p - Protocollo:** parametro, indica quale protocollo bloccare, e per quali macchine o per quali indirizzi IP
- **-s - Sorgente**, da quale indirizzo IP rifiutare, bloccare o lasciar passare qualcosa
- **-i - Interfaccia** da cui facciamo passare, oppure no, qualcosa in ingresso
- **-o - Interfaccia** uscita, a cui si applicano le regole scritte

PER SAPERNE DI PIÙ: http://firestarter.sourceforge.net/

CALENDARI IN LIBERTÁ

7	do	lu	ma	me	gi	ve	sa
8	lu	ma	me	gi	ve	sa	do
9	ma	me	gi	ve	sa	do	lu
10	me	gi	ve	sa	do	lu	ma
11	gi	ve	sa	do	lu	ma	me
12	ve	sa	do	lu	ma	me	gi
13	sa	do	lu	ma	me	gi	ve
14	do	lu	ma	me	gi	ve	sa
15	lu	ma	me	gi	ve	sa	do
16	ma	me	gi	ve	sa	do	lu
17	me	gi	ve	sa	do	lu	ma
18	gi	ve	sa	do	lu	ma	me
19	ve	sa	do	lu	ma	me	gi
20	sa	do	lu	ma	me	gi	ve
21	do	lu	ma	me	gi	ve	sa
22	lu	ma	me	gi	ve	sa	do

IL TEMA-CALENDARIO HA RISCOSSO MOLTO INTERESSE. BRAVI TUTTI! ECCO CHI HA RISPOSTO:

PER TUTTI: Vic (primo arrivato!); VAGABONDO (Ferragosto 1752 fu sabato); Screwy; R.Pryce88 (Pasqua è sempre domenica!); Giorgio Chiesa 89; Impy (visto? Niente indirizzo); PrincipeLele (con il Nokia!); Angelo "Trilussa" Basile; Alessio Failla (manca una w); 4NG3L0, Dark Basic (13 anni!); Glang.; cacciatore-marco2004 (giusto); Lord§Dark; Fox91; Simone Ruggiero (ehm); HnACP; Ras01; TonySnake; figthingfalcon; -=Lyonard=-.

ESPERTI: Neo91; Julian K.; Enrico Sunseri (2004 in base 12 è 11B0, guarda http://www.ex.ac.uk/trol/scol/calnumba.htm) ; PippoPizza (numero più numero meno :-); Microfrog (insomma...); theo-hacker (riscrivici!).

GENI: andrea463 (con carta e penna!); **********************; _Matt_ (e i pirati...); Ar64s-H (dalle vacanze); Fcx (hai ragione!); BioHazard (riprova); Daniele D'Agostino (dai!); Python_coah (più preciso...); check_mate (giorni, non anni).

SUPER HAKER: Na2SO4, Delphi (251 HJ da Ferragosto 2004 a Ferragosto 2014! 6.339 dal 1752 al 2004!); Daniele Midi, VB6 (26 HJ nel 1752, in Italia!); Io & Heike, VB6 (perdonatissimo!); MatteoGeniaccio (http://www.santuari.it/speciali/pasqua/ e http://members.lycos.co.uk/John_Richards/easter.htm); Simonide, VB; nibbio, StarBasic (due programmi); Andrea Piazza, Visual Basic; Muxiox; klaus74, PHP; Mauro Barzaghi, Java; Gasnervino, Java; /Cancel, Python (benissimo così!); CMOS (bravo, http://xoomer.virgilio.it/_XOOM/esongi/calcolopasqua.htm); Il conte di Padova, C (crociato87@fastwebnet.it); Tool462, Javascript; 13c0lp1, Java; drAkan., Perl (per la collaborazione ne riparliamo); Irvin "Edward" Dominin, VB (e Frank Zappa allora?!?); .:HitmaN89:., Pascal; $k4, bash (dov'è?); mauro742, C; -Maker Boy-; L3yArT, Pascal; ema, VB; Luker, C++ (ok così!); Ezio Rizzo (QBasic 4.5); eafkuor, C; Mario Maaroufi (manda pure; per i googlewhack, prossimamente!).

Eccezionalmente, Gran Mogol Terminus59, StarCalc (con lode!).

Al prossimo cyberenigma!

X-3ME NON LASCIA NIENTE AL CASO

Dice ===(X-3mE'89)===:
Riferite ad Alex che la decodifica dell'one-time pad usa lo stesso algoritmo della codifica e quindi non c'è da riprogrammare niente. Sulla casualità, ricordo un trucco che molti programmatori C conosceranno:

```
#include <time.h>

srand((unsigned)time(NULL));
int i=rand();
```

QUAL ERA L'ENIGMA DEL NUMERO 57

Sapendo che Hacker Journal esce un giovedì sì e un giovedì no e salta un numero a Natale e il numero più vicino a Ferragosto è detto di Ferragosto...

PER TUTTI: Che giorno della settimana sarà il 15 agosto 2014? E quando cadrà Pasqua 2014?

PER ESPERTI: In che data sarà in edicola Hacker Journal del ferragosto 2014? Quanti numeri di Hacker Journal usciranno, dal 58 fino al numero di Ferragosto 2014 compresi?

PER GENI: Se Hacker Journal fosse nato il primo giovedì del 1752, quanti numeri avrebbe pubblicato in quell'anno? E quanti ne avrebbe pubblicati fino a questo numero compreso?

PER SUPER HACKER: Chi sa scrivere un programma che calcola le date di uscita di Hacker Journal per qualsiasi anno?

AIUTIAMOCI SUL CYBERENIGMA

- **scrivere con subject Cyberenigma** e il numero della rivista, possibilmente con il titolo del cyberenigma;
- consideriamo il nickname quello in fondo al messaggio; chi non autorizza la pubblicazione del proprio indirizzo non lo vedrà pubblicato;
- inviare la soluzione prima che esca il nuovo numero di HJ (non è necessario, ma è meglio);
- non inviare allegati in formato .exe o .vbs perché vengono eliminati dai nostri filtri antispam. Comprimere sempre i file.
- inviare la mail all'indirizzo nella pagina del cyberenigma.

Grazie a tutti in anticipo!

File Help

Anno 2014 + -

Gen	Feb	Mar	Apr	Mag	Giu	Lug	Ago	Set	Ott	Nov	Dic
2	6	6	3	1	5	3	31	4	2	6	4
16	20	20	17	15	19	17	14	18	16	20	18
30				29		31	28		30		

CODICE SU HM

Tutto il codice dei cyberenigmi viene pubblicato nel CD-ROM inserito in ogni copia del nostro mensile Hackers Magazine!

IL PROSSIMO NUMERO IN EDICOLA IL 21 Ottobre 2004!

CYBERENIGMA

Buon Runedì!

PER UMANI: DOVE SI POSSONO TROVARE SUL WEB QUESTI FONT?
CHE COSA C'È SCRITTO NELLE FRASI CHE SEGUONO?

le risposte a:

guestbook@hackerjournal.it